

5-Point Sovereign AI Audit Checklist

YOUR DATA, YOUR INFRA, YOUR CONTROL

The Shadow Discovery Audit (Technical Phase)

Goal: Quantify the "Ghost" usage and identify hidden data exfiltration points.

Network Traffic Baseline: Identify outgoing traffic to known public AI domains (e.g., OpenAI, Anthropic, DeepSeek) outside sanctioned API endpoints.

Browser Extension Sweep: Audit managed browsers for AI writing assistants or sidebars with "Read All Site Data" permissions.

Expenditure Cross-Check: Review corporate card statements for recurring sub-\$50 charges to AI startups—the primary indicator of "Zombie Economy" sprawl .

Zombie Key Detection: Audit code repositories and local environments for forgotten API keys connected to high-limit credit accounts .

Shadow Data Leak Mapping: Identify if proprietary code, internal memos, or PII has been entered into public LLM chat histories .

The results of your Shadow AI Audit are the first step. The second is securing your perimeter. Connect with us at info@vidai.uk

The Jurisdiction & Sovereignty Audit (Legal Phase)

Goal: Move beyond the "Sovereignty Illusion" to protect your IP from foreign overreach.

Jurisdiction Mapping: Identify if parent companies of AI providers are US-based, triggering **US CLOUD Act** exposure regardless of server location .

Subpoena Risk Assessment: Determine if your data can be accessed by foreign governments without a domestic court order.

Encryption Ownership Check: Verify if the enterprise or the cloud vendor holds the master administrative encryption keys.

Egress Friction Analysis: Calculate the "Exit Tax" (typically ~\$0.09 per GB) required to move proprietary datasets to a different provider .

Residency vs. Sovereignty Gap: Confirm that data "residing" in a London region is legally sovereign and immune to foreign jurisdiction .

The results of your Shadow AI Audit are the first step. The second is securing your perimeter. Connect with us at info@vidai.uk

The FinOps & "Zombie" Spend Audit (Financial Phase)

Goal: Identify and eliminate the "Iteration Tax" and unmanaged AI operational waste.

Token Usage Attribution: Ensure every AI-related API call is traced to a specific departmental cost center rather than a general bucket.

Recursive Loop Monitoring: Audit logs for high-frequency token bursts, indicating an autonomous agent has entered an infinite, costly loop.

License Consolidation: Identify overlapping tools (e.g., disparate coding assistants across teams) to regain volume purchasing power.

"Bill Shock" Kill Switch: Verify the existence of an automated circuit breaker that cuts off runaway agentic workflows before budgets spiral.

Gross Margin Impact Study: Analyze if "hidden" AI costs are currently eroding the gross margins of your core products.

The results of your Shadow AI Audit are the first step. The second is securing your perimeter. Connect with us at info@vidai.uk

The "Lag Tax" & Friction Audit (Operational Phase)

Goal: Diagnose the performance gaps that drive employees to use "Shadow" shortcuts.

Latency Benchmarking: Measure if internal AI gateways add **>200ms** of overhead, as anything slower than public tools encourages employee bypass .

Throughput Stress Test: Verify if current infrastructure can handle **15,000+ concurrent connections** without degrading performance.

Migration Velocity Check: Measure the time required to switch backend model providers; if it takes weeks of refactoring, you are paying a "Velocity Tax" .

Infrastructure Footprint Audit: Compare the compute costs of legacy Python-based gateways against high-density Rust-based fabrics .

Developer Tooling Access: Determine if technical teams have access to local testing tools (like VidaiMock) to prevent "Shadow" testing on public clouds .

The results of your Shadow AI Audit are the first step. The second is securing your perimeter. Connect with us at info@vidai.uk

The August 2026 Compliance Audit (Regulatory Phase)

Goal: Prepare for the "Regulatory Vice Grip" of the EU AI Act and UK Safety Standards.

High-Risk Categorization: Map internal AI use cases (e.g., HR, credit scoring) against **EU AI Act** prohibited or high-risk categories .

"Invisible Processing" Audit: Review AI vendor terms to ensure user data is not being scraped for model training without explicit consent.

UK DfE Safety Standards: Verify that sanctioned tools include robust filtering to prevent "cognitive offloading" and exposure to harmful content .

Full Liability Review: Confirm the enterprise is prepared for fines up to **7% of global turnover** if a "Shadow" tool violates prohibited AI practices .

Active Guardrail Verification: Ensure that data is audited and masked **inside the network** before it breaches the perimeter .

The results of your Shadow AI Audit are the first step. The second is securing your perimeter. Connect with us at info@vidai.uk

About Vidai: The Sovereign AI Fabric

Our Mission

At Vidai, we believe that in the age of Agentic AI, your data shouldn't be a liability—it should be your most valuable equity. Our mission is to end the "Sovereignty Illusion" by providing organizations with the infrastructure required to turn transient AI traffic into private, proprietary enterprise assets.

Our Vision

To turn every AI request into Proprietary Equity

What is VidaiServer?

VidaiServer is a high-density, high-performance AI gateway designed to sit **inside your network perimeter**. It is not another "SaaS Blackbox"; it is a localized infrastructure layer that gives you absolute authority over your AI destiny.

- **Your Data, Your Perimeter:** Vidai audits and masks sensitive PII and IP **inside your VPC** before it ever reaches an external provider. No data is "phoned home" to us; we are the invisible guardrail for your private traffic.
- **High-Density Engineering (Rust):** Unlike bloated Python proxies, our **25MB Rust core** delivers global-scale performance with **<10ms of overhead**. It is built for the high-frequency demands of an Agentic workforce, handling 15,000+ concurrent connections on minimal hardware.
- **Strategic Autonomy:** The **No-Code Model Switchboard** allows you to migrate entire workloads between model providers in **4 seconds**—neutralizing vendor lock-in and the "Innovation Ceiling" of closed ecosystems.
- **Governed Profitability:** A real-time FinOps engine provides granular cost attribution and automated "Kill Switches" to stop bill shock from runaway agents before it impacts your margins.

The results of your Shadow AI Audit are the first step. The second is securing your perimeter. Connect with us at info@vidai.uk